

In response to the Official Action mailed July 12, 2007, please amend the claims to read as follows.

1 1. (currently amended) In a data processing operation  
2 having stored data in a plurality of data files, a system  
3 for protecting said data files from unauthorized users  
4 comprising:  
5 means for storing for each of said plurality of data  
6 files, a backup file inaccessible to user requests;  
7 means for receiving user requests for access to data  
8 files;  
9 means for determining, without accessing any of said  
10 backup files, whether said requests are unauthorized  
11 intrusions into said requested data files;  
12 means responsive to an initial determination that a  
13 request is unauthorized for destroying the requested data  
14 files; and  
15 means for reloading a backup file for each destroyed  
16 file.

2-3. (cancelled).

1 4. (original) The data processing operation system of claim  
2 1 wherein said means for determining whether said user  
3 requests are unauthorized intrusions include:  
4 means for determining whether a user access identifica-  
5 tion code has been denied; and  
6 means for determining whether the user has copied the  
7 requested files.

1 5. (currently amended) In a communication network with  
2 access to a plurality of network sites each having stored  
3 data in a plurality of data files accessible in response to  
4 requests from users at other sites in the network, a system  
5 for protecting said network site data files from unautho-  
6 rized users comprising:

7 means for storing for each of said plurality of data  
8 files at said network site, a backup file inaccessible to  
9 user requests;

10 means associated with a network site for  
11 receiving user requests for access to data files;

12 means at said network site for determining, without  
13 accessing any of said backup files, whether said user  
14 requests are unauthorized intrusions into said requested  
15 data files;

16 means at said network site responsive to an initial  
17 determination that a request is unauthorized for destroying  
18 the requested data files; and

19 means for reloading a backup file for each destroyed  
20 file.

6. (cancelled)

1 7. (currently amended) In a World Wide Web communication  
2 network with access to a plurality of open Web sites each  
3 having stored data in a plurality of data files accessible  
4 in response to requests from users at stations throughout  
5 the Web, a system for protecting said open Web site data  
6 files from unauthorized users comprising:  
7 means for storing for each of said plurality of data  
8 files at said open Web site, a backup file inaccessible to  
9 user requests;  
10 means associated with an open Web site for  
11 receiving user requests for access to data files;  
12 means at said open Web site for determining, without  
13 accessing any of said backup files, whether said user  
14 requests are unauthorized intrusions into said requested  
15 data files;  
16 means at said open Web site responsive to an initial  
17 determination that a request is unauthorized for destroying  
18 the requested data files; and  
19 means for reloading a backup file for each destroyed  
20 file.

8-9. (cancelled).

1 10. (currently amended) In a data processing operation  
2 having stored data in a plurality of data files, a method  
3 for protecting said data files from unauthorized users  
4 comprising:  
5 storing for each of said plurality of data files, a  
6 backup file inaccessible to user requests;  
7 receiving user requests for access to data files;  
8 determining, without accessing any of said backup  
9 files, whether said requests are unauthorized intrusions  
10 into said requested data files;  
11 destroying the requested data files responsive to an  
12 initial determination that a request is unauthorized; and  
13 reloading a backup file for each destroyed file.

11-12. (cancelled).

1 13. (original) The data processing method of claim 10 where-  
2 in said step of determining whether said user requests are  
3 unauthorized intrusions includes:  
4 determining whether a user access identification code  
5 has been denied; and  
6 determining whether the user has copied the requested  
7 files.

1 14. (currently amended) In a communication network with  
2 access to a plurality of network sites each having stored  
3 data in a plurality of data files accessible in response to  
4 requests from users at other sites in the network, a method  
5 for protecting said network site data files from  
6 unauthorized users comprising:  
7 storing for each of said plurality of data files at  
8 said network site, a backup file inaccessible to user re-  
9 quests;  
10 receiving user requests for access to data files at a  
11 network site;  
12 determining at said network site, without accessing any  
13 of said backup files, whether said user requests are  
14 unauthorized intrusions into said requested data files;  
15 destroying the requested data files responsive to an  
16 initial determination that a request is unauthorized; and  
17 reloading a backup file for each destroyed file.

15-16. (cancelled).

1 17. (currently amended) In a World Wide Web communication  
2 network with access to a plurality of open Web sites each  
3 having stored data in a plurality of data files accessible  
4 in response to requests from users at stations throughout  
5 the Web, a method for protecting said open Web site data  
6 files from unauthorized users comprising:  
7 storing for each of said plurality of data files at  
8 said open Web site, a backup file inaccessible to user  
9 requests;  
10 receiving user requests for access to data files at  
11 said open Web site;  
12 determining, without accessing any of said backup  
13 files, whether said user requests are unauthorized  
14 intrusions into said requested data files at said open Web  
15 site;  
16 destroying the requested data files at said open Web  
17 site responsive to an initial determination that a request  
18 is unauthorized; and  
19 reloading a backup file for each destroyed file.

18-19. (cancelled).

1 20. (original) The World Wide Web communication network  
2 method of claim 17 wherein said step of determining whether  
3 said user requests are unauthorized intrusions includes:  
4 determining whether a user access identification code  
5 has been denied; and  
6 determining whether the user has copied the requested  
7 files.

21-30. (cancelled).

PATENT  
09/801,614

1 31. (new) A computer readable medium having stored thereon a  
2 computer readable program for protecting data stored in a  
3 plurality of data files from unauthorized users, wherein the  
4 computer readable program when executed on a computer causes  
5 the computer to:  
6       store for each of said plurality of data files, a  
7 backup file inaccessible to user requests;  
8       receive user requests for access to data files;  
9       determine, without accessing any of said backup files,  
10 whether said requests are unauthorized intrusions into said  
11 requested data files;  
12       destroy the requested data files responsive to an  
13 initial determination that a request is unauthorized; and  
14       reload a backup file for each destroyed file.

1 32. (new) The computer readable medium of claim 31, wherein  
2 in determining whether said user requests are unauthorized  
3 intrusions, the computer readable program causes the  
4 computer to:  
5       determine whether a user access identification code has  
6 been denied; and  
7       determine whether the user has copied the requested  
8 files.

1 33. (new) A computer readable medium having stored thereon a  
2 computer readable program for protecting, from unauthorized  
3 users, data stored in a plurality of data files at network  
4 sites accessible in response to requests from users at other  
5 sites in the network, wherein the computer readable program  
6 when executed on a computer causes the computer to:  
7       store for each of said plurality of data files at said  
8 network site, a backup file inaccessible to user requests;  
9       receive user requests for access to data files at a  
10 network site;  
11       determine at said network site, without accessing any  
12 of said backup files, whether said user requests are  
13 unauthorized intrusions into said requested data files;  
14       destroy the requested data files responsive to an  
15 initial determination that a request is unauthorized; and  
16       reload a backup file for each destroyed file.

1 34. (new) The computer readable medium of claim 33, wherein  
2 the network is the World wide Web and said network sites are  
3 Web sites.

1 35. (new) The computer readable medium of claim 34, wherein  
2 in determining whether said user requests are unauthorized  
3 intrusions, the computer readable program causes the  
4 computer to:  
5       determine whether a user access identification code has  
6 been denied; and  
7       determine whether the user has copied the requested  
8 files.